CLAIMS

What is claimed is:

1. A method of authenticating a subject, comprising:

using one or a plurality of biometric measurements for authentication without any sharing of the subject's biometric data.

2. The method according to claim 1, further comprising:

storing said biometric data in an individual unit, said individual unit belonging to said subject.

3. The method according to claim 2, wherein said individual unit is portable for being carried by said subject.

4. The method according to claim 2, wherein said individual unit is non-portable.

5. The method according to claim 2, wherein said individual unit comprises one of a smart card, a personal area network (PAN) tool, and an apparatus linked to a network.

6. The method according to claim 1, further comprising:

after said authentication, selectively obtaining access to any of a location, a service, and an option in a service by said subject.

7. The method according to claim 1, further comprising:

generating at least one of a password and another authentication procedure based on biometric authentication locally under the subject's control.

8. The method according to claim 7, further comprising:

securely storing the biometric on an apparatus carried by said subject.

9. The method according to claim 1, further comprising:

generating at least one of a password and another authentication procedure based on at least one biometric feature extracted locally under the subject's control.

10. The method according to claim 9, wherein said generating is performed without storing the subject's biometric feature.

11. The method according to claim 9, further comprising:

deriving said at least one of the password and the another authentication procedure from the biometric extracted locally when authentication is required.

12. The method according to claim 7, further comprising:

deriving said at least one of the password and the another authentication procedure from compressed biometrics extracted locally under the subject's control or from a network, when authentication is required.

13. The method according to claim 7, further comprising:

managing multiple passwords and authentication procedures, by at least one of:

monitoring an authentication request;

identifying a requestor;

generating at least one of a new password and an authentication procedure for a new requester;

storing the authentication procedure generation method and the identity of the requestor in a secure manner; and

authenticating the user for known requesters using the stored procedure and the result of the local authentication procedure.

14. A method of authenticating a characteristic of a subject, without compromising privacy of the subject, comprising:

using at least one of a plurality of authentication methods including personal information of the subject, a biometric of the subject, a password, a personal identification number (PIN) and a secured component; and

simultaneously with said using, said subject maintaining confidentiality of authentication information and withholding said authentication information from the other party.

15. The method according to claim 14, further comprising:

generating at least one of a password and another authentication procedure based on authentication locally under the subject's control.

16. The method according to claim 15, further comprising:

securely storing authentication information on an apparatus locally under the subject's control.

17. The method according to claim 15, further comprising:

deriving said at least one of the password and the another authentication procedure from the local authentication when authentication is required.

18. The method according to claim 16, further comprising:

securely storing the authentication information on the apparatus using at least one of a knowledge-based information, a possession-based information, a password-based information, and a biometric-based information.

19. The method according to claim 14, further comprising:

selectively completing the authentication with a remote service using a communication port and protocol.

20. A method for secure authentication of a subject, comprising:

selectively requesting any of a password and a knowledge-based information from said subject; and

simultaneously with said selectively requesting, interrogating biometric information of the subject, said biometric information being carried by said subject.

21. The method according to claim 20, further comprising:

using said biometric information to generate said password.

22. The method according to claim 20, further comprising:

performing biometric data verification by a device associated with said subject,

wherein said biometric data verification activates a password-controlled authentication mechanism which transfers information, but which withholds sufficient information so that the biometric is not revealed, to a party requiring authentication.

23. The method according to claim 21, wherein obtaining said password is

performed by using at least one of an encryption and secure hashing.

24. The method according to claim 20, wherein a device is carried by the subject to be authorized to perform a task,

wherein at a moment of authorization, said device is presented to a reader of an authorizing machine of an entity seeking authentication, which prompts said device for a password for authorization to be given, and

wherein said device reads a biometric of said subject using a sensor included in the device and computes the password.

25. The method according to claim 24, wherein said device allows the password to be read by the authorizing machine.

26. The method according to claim 25, wherein said password is read in a contacting manner.

27. The method according to claim 25, wherein said password is read in a contact-free manner.

28. The method according to claim 24, further comprising:

using one of a hashing and a mapping technique, which is stable with respect to variations of the biometric extracted, said using including mapping regions of a biometric-print space, to the password having been computed.

29. The method according to claim 28, wherein said using includes:

measuring a biometric-print of the subject by ranking biometric prints of N subsets of M biometrics,

wherein an index of a top ranking of each of the N subsets is used in computing the password.

30. The method according to claim 24, further comprising:

storing on the device information regarding a previous authentication including a biometric-print of the subject.

31. The method according to claim 20, further comprising:

encrypting a biometric-print using the subject's biometric and personal knowledge onto a device carried by said subject.

32. The method according to claim 20, further comprising:

providing a unique non-duplicable authentication mechanism on a device associated with said subject, said authentication mechanism being constructed so as to be completely independent of the biometric,

wherein said authentication mechanism is prevented from accessing the biometric itself.

33. The method according to claim 32, wherein said device associated with

said subject produces a correct password only when the device reads a biometric from the subject.

34. The method according to claim 20, wherein biometric information for a plurality of subjects is stored in a device associated with the subject.

35. An apparatus for secure authentication, without compromising privacy of a subject, comprising:

a reader, associated with the subject, for reading a specified biometric of said subject; and

a password generator for producing a password needed based on said biometric.

36. The apparatus according to claim 35, wherein said password generator includes an encryption device using at least one of encryption and secure hashing.

37. An apparatus for secure authentication, comprising:

means, associated with a subject, for reading a specified biometric of said subject; and

means for producing a password needed based on said biometric, without providing access to said biometric by anyone other than said subject.

38. The apparatus according to claim 37, wherein said means for producing said password includes an encryption device using at least one of encryption and secure hashing.

39. A method of identifying a subject, comprising:

using one or a plurality of biometric measurements for identification without any sharing of the subject's biometric data.

40. The method of claim 39, wherein a subject's identity is determined locally, under the subject's control, by having the subject provide at least one of a user ID and by biometric identification of the subject among enrolled authorized subjects, and

wherein said identification produces a set of N best matches for N subsets, and an index formed by concatenation of the N indices uniquely identifies the subject.

41. A method for identification of a subject, comprising:

selectively requesting any of a password and a knowledge-based information from said subject; and

simultaneously with said selectively requesting, interrogating biometric information of the subject, said biometric information being carried by said subject.

42. The method of claim 41, wherein a subject's identity is determined locally, under the subject's control, by having the subject provide at least one of a user ID and by biometric identification of the subject among enrolled authorized subjects, and

wherein said identification produces a set of N best matches for N subsets, and an index formed by concatenation of the N indices uniquely identifies the subject.

43. An apparatus for identification of a subject, comprising:

a reader, associated with the subject, for reading a specified biometric of said subject; and

a password generator for producing a password needed based on said biometric.

44. The apparatus according to claim 43, further comprising:

means for storing data of said biometric in an individual unit, said individual unit belonging to said subject.

45. The apparatus according to claim 44, wherein said individual unit is portable for being carried by said subject.

46. The apparatus according to claim 44, wherein said individual unit is non-portable.

47. The apparatus according to claim 44, wherein said individual unit comprises one of a smart card, a personal area network (PAN) tool, and an apparatus linked to a network.

48. The apparatus according to claim 44, wherein a subject's identity is determined locally, under the subject's control, by having the subject provide at least one of a user ID and by biometric identification of the subject among enrolled authorized subjects being read by said reader, and

wherein said identification produces a set of N best matches for N subsets, and an index formed by concatenation of the N indices uniquely identifies the subject.